AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

Claim 1 (Previously Presented): A method of anti-virus processing an email having an executable attachment comprising the steps, executed by a machine, of:

a)   extracting structural elements from the email;

b)   examining the executable attachment and comparing the executable attachment with the extracted structural elements to determine whether the executable attachment contains code, data or encoded data that could have created the extracted structural elements; and

c)   signalling that the attachment is possibly viral or not on the basis of the extent to which the examining step b) finds evidence that the structural elements have been created by that attachment.

Claim 2 (Original): A method according to claim 1, wherein the structural elements are categorised and the step c) includes assigning a numeric score for each

element which could have been created by that attachment, and signalling that the attachment is possibly viral or not on the basis of an overall score.

Claim 3 (Original): A method according to claim 2, wherein the scores are weighted according to category.

Claim 4 (Previously Presented): A method according to claim 1, wherein the signalling step c) takes account of factors including any or all of the following attributes of the email:

standard MIME headers;

unusual MIME headers;

deviations from RFC standards;

unusual constructs;

number of attachments;

type of attachments;

encoding method used for attachments;

text content of the email; and

HTML or XHTML content of the email.

Claim 5 (Previously Presented): A method according to claim 1, wherein the step a) includes extracting the structural elements as strings, the step b) includes

examining the attachments for matches of those strings and the step c) signals the attachment as possibly viral or not on the basis of the extent to which the examining step b) finds occurrences of the strings in the attachment.

Claim 6 (Previously Presented):   A system for anti-virus processing an email having an executable attachment comprising the following means, implemented by a machine:

a)   means for extracting structural elements from the email;

b)   means for examining the executable attachment and comparing the executable attachment with the extracted structural elements to determine whether the executable attachment contains code, data or encoded data that could have created the extracted structural elements; and

c)   means for signalling that the attachment is possibly viral or not on the basis of the extent to which the examining step b) finds evidence that the structural elements have been created by that attachment.

Claim 7 (Original):   A system according to claim 6, wherein the structural elements are categorised and the means c) includes means for assigning a numeric score for each element which could have been created by that attachment, and signalling that the attachment is possibly viral or not on the basis of an overall score.

Claim 8 (Original): A system according to claim 7, wherein the scores are weighted according to category.

Claim 9 (Previously Presented): A system according to claim 6, wherein the means c) takes account of factors including any or all of the following attributes of the email:

standard MIME headers;

unusual MIME headers;

deviations from RFC standards;

unusual constructs;

number of attachments;

type of attachments;

encoding method used for attachments;

text content of the email; and

HTML or XHTML content of the email.

Claim 10 (Previously Presented): A system according to claim 6, wherein the means a) extracts the structural elements as strings, the means b) examines the attachments for matches of those strings and the means c) signals the attachment as possibly viral or not on the basis of the extent to which the means b) finds occurrences of the strings in the attachment.

Claim 11 (Previously Presented): A method of anti-virus processing an email having an executable attachment comprising the steps, executed by a machine, of:

a)   extracting structural elements from the email;

b)   examining the executable attachment for code, data or encoded data that could have created the extracted structural elements; and

c)   signalling that the attachment is possibly viral or not on the basis of the extent to which the examining step b) finds evidence that the structural elements have been created by that attachment,

wherein the step a) includes extracting the structural elements as strings, the step b) includes examining the attachment for matches of those strings and the step c) signals the attachment as possibly viral or not on the basis of the extent to which the step b) finds occurrences of the strings in the attachment.

Claim 12 (Previously Presented): A computer readable medium having stored thereon instructions for causing a computer to carry out a method of processing an email having an executable attachment, the method comprising:

a)   extracting structural elements from the email;

b)   examining the executable attachment and comparing the executable attachment with the extracted structural elements to determine whether the executable

attachment contains code, data or encoded data that could have created the extracted structural elements; and

c)   signalling that the attachment is possibly viral or not on the basis of the extent to which the examining finds evidence that the structural elements have been created by that attachment.

Claim 13 (Previously Presented): A system comprising the computer-readable medium according to claim 12.

Claim 14 (New):   The computer readable medium according to claim 12, wherein the extracting extracts the structural elements as strings, the examining examines the attachment for matches of those strings and the signaling signals the attachment as possibly viral or not on the basis of the extent to which the examining finds occurrences of the strings in the attachment.